Please type a plus sign (+) inside this box → [+]

#4

PTO/SB/08A (08-00)
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	09/621,056
Filing Date	July 21, 2000
First Named Inventor	Carman
Group Art Unit	2766
Examiner Name	To be assigned
Attorney Docket Number	NTWK005/05US

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	U.S. Patent Document Number	Kind Code[2] (if known)	Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
TH	A1	5,724,428		Rivest	03-03-98	
TH	A2	5,835,600		Rivest	11-10-98	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Office[3]	Number[4]	Kind Code[5] (if known)	Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
	B1							
	B2							

OTHER PRIOR ART – NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
TH	C1	M. BELLARE, R. CANETTI, and H. KRAWCZYK, "Keying Hash Functions for Message Authentication" in *Advances in Cryptology: Proceedings of CRYPTO '96*, LNCS 1109, N. Koblitz, ed., Springer-Verlag (1996), 1–15.	
TH	C2	R. CANETTI, J. GARAY, G. ITKIS, D. MICCIANCIO, M. NAOR, and B. PINKAS, "Multicast Security: A Taxonomy and Efficient Constructions" in *INFOCOM '99 Proceedings*, March 1999.	
TH	C3	P. ROGAWAY, "Design and Analysis of Message Authentication Codes," presented at the 1996 RSA Data Security Conference, January 19, 1996.	
TH	C4	P. ROGAWAY, "Bucket Hashing and its Application to Fast Message Authentication,", J. of Cryptology, October 13, 1997.	
TH	C5	J. TOUCH, "Performance Analysis of MD5," proceedings of Sigcomm '95, Boston, MA.	
TH	C6	Atomic-2 Fast Security, http://www.isi.edu/atomic2/security/, printed January 15, 2001.	
TH	C7	Cryptographic Technologies Adaptive Cryptographically Synchronized Authentication (ACSA), http://www.pgp.com/research/nailabs/cryptographic/adaptive-cryptographic.asp, printed January 12, 2001.	
TH	C8	D. Balenson, et al. , ACSA Kickoff Brief presented to DARPA on September 11, 1998.	
TH	C9	D. Balenson, et al., ACSA Presentation to the DARPA/ITO Next Generation Internet (NGI) Principal Investigator's (PI) Meeting held on October 29, 1998.	
TH	C10	D. Balenson, et al. ACSA Presentation to the XIWT Workshop on Information Assurance and Trustworthy Networks held November 18, 1998.	
TH	C11	D. Carmen, "Adaptively Trading Off Strength and Performance in Network Authentication," Presentation at the RSA Conference 2000 held January 19, 2000.	
TH	C12	D. Balenson, et al., ACSA Model and Analysis Document – Revision 1.0 delivered to DARPA on December 7, 1998.	
TH	C13	D. Carmen, et al., ACSA Prototype System Design Document, Revision 1.0, May 12, 1999	

[1]

[2] See attached Kinds of U.S. Patent Documents.
[3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3).
[4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document.
[5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible.
[6] Applicant is to place a check mark here if English language Translation is attached.

#9

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet	2	of	2

Complete if Known	
Application Number	09/621,056
Filing Date	July 21, 2000
First Named Inventor	Carman
Group Art Unit	2766
Examiner Name	To be assigned
Attorney Docket Number	NTWK005/05US

RECEIVED
JUN 29 2001
Technology Center 2100

OTHER PRIOR ART – NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[1]
TH	C14	D. Carmen, et al., ACSA Final Report delivered to DARPA on December 6, 2000.	
TH	C15	DARPA ITO Sponsored Research, 1998 Project Summary, Adaptive Cryptographically Synchronized Authentication.	
TH	C16	DARPA ITO Sponsored Research, 1999 Project Summary, Adaptive Cryptographically Synchronized Authentication.	
TH	C17	J. BLACK, S. HALEVI, H. KRAWCZYK, T. KROVETZ, and P. ROGAWAY, "UMAC: Fast and Secure Message Authentication," Advances in Cryptology - CRYPTO '99, vol. 1666, Springer-Verlag, 1999, pp. 216-233.	
TH	C18	J. ADCOCK, D. BALENSON, D. CARMAN, M. HEYMAN, and A. SHERMAN, "Trading Off Strength and Performance in Network Authentication: Experience with the ACSA Project," DARPA Information Survivability Conference and Exposition, January 25-27, 2000.	
TH	C19	Department of Defense Security Institute, STU-III Handbook for Industry, February 1997.	
TH	C20	Commerce Business Daily, PSA#2134, July 10, 1998.	
TH	C21	R. GENNARO and P. ROHATGI, "How to Sign Digital Streams," In Proceedings of CRYPTO 97, pages 180--197, February 24, 1998, Santa Barbara, CA.	
TH	C22	S. HALEVI and H. KRAWCZYK, "MMH: Software message authentication in the Gbit/second rates," Fast Software Encryption, LNCS 1267, E. Biham, Ed., Springer-Verlag, 1997, pp. 172--189.	
TH	C23	D. MCGREW, "Optimal One-Time Signature Methods," Trusted Information Systems Technical Report, August, 1997.	
TH	C24	H. KRAWCZYK, "LFSR-Based Hashing and Authentication," In Proc. CRYPTO 94, Lecture Notes in Computer Science. Springer-Verlag, 1994.	
TH	C25	Wegman, et al. "New Hash Functions and Their Use in Authentication and Set Equality," J Computer and System Services, (1981), 22:265-279	

Examiner Signature	Thomas Ho	Date Considered	2/09/04

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

101006 v1/RE
25XQ01!.DOC
062801/1439